ITS Technical Bulletin

# TB-0354

## Network Perimeter Security Enhancements

| | |
|---|---|
| Issue Date: | Month 00, 2000 |
| Effective Date: | January 9, 2005 |
| Section/Group: | Enterprise Information Security Office |
| Submitted by: | Michael Allred |
| Approved by: | Ken Elliot |

In December 2003, ITS Technical Bulletin #332: *Enhanced Security Requirements for System Access* was issued to close down port 23 (Telnet) on the perimeter firewall. The Security Office has received a good deal of support for this, and hundreds of conduits have been eliminated. We continue to work with those State and local agencies to eliminate all clear text external access.

As part of our ongoing effort to enhance the security of the State of Utah's perimeter defenses, effective January 9, 2005, **incoming traffic** to the following ports will be closed at the perimeter firewall.

| Ports | Usage | | Ports | Usage |
|---|---|---|---|---|
| 22 | Used for Secure Shell (SSH) | | 5800 | VNC default port for client |
| 55 | VNC Servers | | 5850 | Unspecified |
| 123 | Network Time Protocol (NTP) | | 5900 | VNC default port for Web client |
| 443 | Used for SSL access to Web site | | 5950 | Unspecified |
| 7100 | TCP—font-service | | 5955 | Unspecified |
| 8009 | Novell Remote Manager | | 5631 | PCAnywhere |
| 8081 | Unspecified | | 5632 | PCAnywhere |
| 4900 | MUTE file sharing (like Kazaa) | | | |

Today these ports allow *any* computer in the world to access *any* computer on the State network.  We are making a concerted effort to move toward a policy of "***deny that that***

***is not specifically allowed.*** ” To do this we are eliminating conduits that allow for *any* external access to *any* internal address.

If an agency needs specific access lists built for these ports, the agency’s security officer must submit a list of ***source and destination*** IP address that they need to remain open. The request should be sent to **dsecure@utah.gov** and include the IP addresses to remain open, a contact name, phone number, e-mail address, and a brief reason that will be used for tracking. This must be done prior to the January 9th dead line. Multiple requests may be submitted with one e-mail.

After the January 9, 2005, a standard firewall request form will be used to allow these ports to be open.

**Alternatives**

It is recommended that agencies look at alternative methods to support internal systems. Using VPN or some method to require authentication prior to network access is encouraged. This allows the State to minimize the number of ACLs the firewall has to support and increases the security of the systems. The Security Office also encourages State agencies to be aware of additional security risks associated with allowing external access to servers and desktops on the State network. Remote control programs, like VNC, PCAnywhere, gotomypc, and terminal services, can be great productivity tools for local administrators, but they can also be used by external sources to compromise the State network. They should be used sparingly and monitored constantly.

**The information in this bulletin is considered confidential and not for external distribution**.